

Exhibit Q

KANNER & WHITELEY, L.L.C.**701 Camp Street****New Orleans, Louisiana 70130****(504) 524-5777****FAX: (504) 524-5763**

November 11, 2019

Via Email

Seth A. Goldberg, Esq.
Duane Morris LLP
30 South 17th Street
Philadelphia, PA 19103-4196
SAGoldberg@duanemorris.com

RE: *In re Valsartan Products Liability Litigation*, No. 1:19-md-02875
(In-Person ESI Meet-and-Confers)

Counsel:

I write further to Adam Slater's letter of April 8, 2019, and Paragraph 6 of the Court's November 7, 2019, Order ("Court's Order"). (D.E.292)

While Plaintiffs continue to seek all the documents and information set forth in their April 8, 2019, letter, in the interests of efficiency and in advance of the in-person meetings, Plaintiffs provide a more tailored set of topics below.

Plaintiffs have identified this narrowed (and sometimes more specific) set of topics as those most pertinent to the anticipated meetings with Defendants' persons most knowledgeable regarding their information management and related systems.¹ *See* Court's Order at ¶ 6. Plaintiffs note that the below is not an exhaustive list of inquiries, but, rather, is being provided in a good-faith effort to frame the issues Plaintiffs expect to discuss so that Defendants may identify the appropriate person(s) most knowledgeable.

A. Document Retention Policies

1. Describe the document retention and/or records management policies and procedures for each defendant with respect to documents responsive to Plaintiffs' Requests for the Production of Documents ("RFPDs").

¹ Plaintiffs acknowledge (and appreciate) that some Defendants have already begun the process of providing specific information regarding the software programs and structured data systems used to create and store electronic documents in the ordinary course of business. This information will be instructive for the in-person meetings.

2. Confirm whether any documents that are relevant to any of the issues in this litigation have been destroyed, discarded, or are otherwise no longer available, and documentation of efforts to make this determination.
3. Describe policies related to the preservation of the desktops/laptops/mobile devices/data/documents/information of former relevant employees and the data therein, including but not limited to any custodians identified by Plaintiffs or Defendants.

B. Internal Company Files

1. Produce a list of all potential sources and locations of paper documents that are relevant to the issues in this litigation.
2. Provide the earliest date on which documents related to the drugs at issue exists in each defendant's files.
3. Produce a list of all file types and extensions that actually appear and/or exist in the names of or within files **that contain relevant documents**, including but not limited to relevant emails or other communications, and identify the software used to create and/or access such files.

C. Technology Assisted Review ("TAR") and Search Terms

1. Confirm whether defendants have used or intend to use TAR (including predictive coding) for searching, locating, determining the relevancy of, or review of documents.

D. Network Servers

1. Describe any network or server based system and topology utilized by defendants for any information systems potentially containing documents responsive to Plaintiffs' RFPDs and provide documentation describing:
 - a. The number and types of computers/servers utilized and their locations.
 - b. All operating systems installed on any computers/servers.
 - c. All software applications used at any time during the relevant time frame.
2. Describe all intranets, communications systems, file storage systems, document management systems, and database systems accessible to any employees that may contain, or have contained, potentially relevant information during the entire relevant time period.
3. Confirm whether the company maintains servers at any of the company's divisions/business units/locations/offices/subsidiaries/affiliates/vendors that exist

separately from or in addition to company-wide server(s), and if so, describe to what extent any of those servers may store any potentially relevant information.

4. Produce any index, network topology, or ESI Data map that exists of defendants' IT systems.
5. Identify all computers, equipment, devices, or servers on which data responsive to Plaintiffs' RFPDs did exist, but for which data no longer exists due to a computer, equipment, device, or server crash; intentional or unintentional deletion of data; or destruction or disposition of the computer, equipment, device, or server.
6. Identify all computers, equipment, devices, or servers on which any relevant testing data is or was kept.
7. Describe the backup system of each of defendants' computers, servers, workstations, and devices (by category) and provide documentation describing the following:
 - a. Identification of what data is backed up.
 - b. The dates for which backup data is available.
 - c. Backup schedules.
 - d. Identification of any of any third-party backup/storage/archiving product or location utilized by defendants.
 - e. The format of the backup, including but not limited to the type of media on which such backups are stored, and the location of such media.

E. Email/Messaging/Communications Servers/Systems

1. Identify the systems used for any exchange of communications by your employees, including but not limited to email, instant messaging, text messaging, imessaging, SMS, MMS, chat rooms, list-servers, discussion forums, voicemail, voice-chat, video-chat, video-conferencing, and shared data stores, and the time period for the use of each system, including any systems used at any overseas facilities; and provide documentation describing the following:
 - a. Server, workstation, and device name, software and version.
 - b. Location of communication files.
 - c. All software and/or applications used on such systems.
2. Identify communications servers at any or all of the company's divisions/business units/locations/offices/subsidiaries that exist separately or in addition to the company-wide server(s).
3. Indicate whether any end-user communications are stored on (i) the end-user's hard drive, (ii) servers, (iii) a server of a third-party application service provider, or (iv) a mobile device.

4. If any of defendants' communications systems have changed during the relevant time period, identify any legacy system(s), the current system(s), the date range for which information is available on each system, and the date(s) of the backup(s) made with each relevant legacy system.
5. Describe the backup system of each of defendants' communications servers and devices and provide documentation describing the following:
 - a. Identification of what data and information is backed up.
 - b. The dates for which backup data is available.
 - c. Backup schedules.
 - d. Identification of any third-party backup/storage/archiving product utilized by defendants.
 - e. The format of the backup, including but not limited to the type of media on which such backups are stored, and the location of such media.
6. Produce all company policies related to how employees access their email and other communications on mobile devices or personal devices and provide a description of how the data from the mobile device and email or other communications client are synced.

F. Hard Drives/Devices

1. Produce all company policies governing the backup of employees' desktop and laptop hard drives and other devices, including but not limited to cellphones, smartphones, tablets, USB drives, and PDAs.
2. Describe defendants' efforts to determine the extent to which any of the key custodians in this litigation have relevant information which is located on such hard drives and other devices.
3. Confirm whether at any time such hard drives and other devices were or are erased, "wiped," "scrubbed," or reformatted.
4. Produce all company policies related to "approved" communication applications, including but not limited to text messaging/instant messaging applications or other third-party applications such as Salesforce.com or Slack.

G. Non-Company Computers/Devices

1. Produce all company policies governing employee use of computers or other devices not owned or controlled by the company to create, receive, store, or send work-related documents or communications.
2. Identify all third-party systems and applications, including but not limited to cloud-based systems and applications, that may contain relevant data, and all policies and procedures that are relevant thereto.

3. Produce all documentation relating to any BYOD (“Bring Your Own Device”) policy in place.

Plaintiffs do not provide the above as a waiver of their rights to compel production of any documents and/or information identified in their April 8, 2019, letter. Indeed, Plaintiffs disagree with Defendants’ objections² that the information Plaintiffs requested is overly broad, unduly burdensome or not relevant to any party’s claims or defense. *See* Brancato November 5, 2019, letter on behalf of all Defendants at 3.

Nevertheless, Plaintiffs hope the more narrowly tailored list of items (much of which consists of information Defendants have already agreed to provide)³ will hopefully facilitate a productive conversation between the Parties, as well as with Defendants’ person most knowledgeable.

Plaintiffs look forward to meeting with Defendants later this week.

Sincerely,

KANNER & WHITELEY, L.L.C.

By:



Layne C. Hilton

Cc: Jessica Priselac, Esq. (*via email*) (to distribute to all Defendants)
Plaintiffs’ Co-Leads (*via email*)
Plaintiffs’ PEC (*via email*)

² Plaintiffs note that Defendants took almost *seven months* to provide their written objections in response to Plaintiffs’ April 8, 2019, letter. Arguably, Defendants’ objections are not timely. That having been said, Plaintiffs are committed to working through any issues in a cooperative manner.

³ Prior to the Court’s order, Defendants previously agreed to provide information regarding: i) use of TAR, ii) ability to run search terms across electronic sources, iii) non-company computers or devices, iv) backup, storage and archiving, network servers, and v) email, messaging and communication servers and systems. *See* Brancato November 5, 2019, letter on behalf of all Defendants.